IN THE CLAIMS

1-7 (cancelled)

8. (previously presented) A playback method for decrypting encrypted data read from a recording medium, comprising the steps of:

when a player is going to play back the recording medium containing user identification information, intended to identify a user, and data encrypted with the user identification information, causing the player to detect whether a terminal unit with a memory having the user identification information recorded therein along with the data is connected to the player;

when it is detected that the terminal unit is connected to the player, exchanging an encryption key between the player and the terminal unit;

encrypting the user identification information read from the memory of the terminal unit with the exchanged encryption key and sending it from the terminal unit to the player;

judging whether the user identification information sent from the terminal unit is coincident with the user identification information read from the recording medium; and

decrypting the encrypted data read from the recording medium when it is judged that the user identification information sent from the terminal unit is coincident with the user identification information read from the recording medium.

9. (previously presented) The method according to claim 8, wherein when it is judged that the user identification information sent from the terminal unit is not coincident with the user identification information read from the recording medium, output of data read from the recording medium is inhibited.

10. (previously presented) The method according to claim 8, wherein:

when it is detected that the terminal unit is connected to the player, the player authenticates the terminal unit; and

when the player has not successfully authenticated the terminal unit, output of data read from the recording medium is ceased.

11. (previously presented) The method according to claim 10, wherein when the player has not successfully authenticated the terminal unit, an error message is displayed.

12. (original) The method according to claim 8, wherein when it is detected that the terminal unit is not connected to the recorder, a display is made to indicate that the terminal unit is not connected.

13. (previously presented) The method according to claim 8, wherein the user identification information stored in the memory of the terminal unit is set by the user.

14. (original) The method according to claim 13, wherein the user identification information includes a user name.

15. (original) The method according to claim 14, wherein the user identification information includes information unique to the terminal unit, having been set at the time of shipment from factory.

16 – 17. (cancelled)

18. (currently amended) A method of playing back a recording medium, comprising:

when a player is going to play back a recording medium containing user identification information, intended to identify a user, and data having been encrypted

with the user identification information and stored in the recording medium therewith, judging whether user identification information read from an information holder provided in the player to hold user identification information sent from a terminal unit is coincident with user identification information read from the recording medium;

decrypting encrypted data read from the recording medium when the user identification information read from the information holder provided in the player is coincident with the user identification information read from the recording medium; and

~~The method according to claim 16, wherein:~~

~~when the terminal unit is connected to the player,~~ exchanging an encryption key ~~is exchanged~~ between the player and terminal unit when the terminal unit is connected to the player;

encrypting the user identification information read from the memory of the terminal unit ~~is encrypted~~ with the exchanged encryption key; and

~~sent~~ sending the encrypted user identification information from the terminal unit to the player.

19-25 (cancelled)

26. (previously presented) A data transmitting method, comprising the steps of:

when an output unit to output data read from a recording medium having data recorded therein that includes user identification information intended to identify a user and data which has been encrypted with the user identification information is going to output data read from the recording medium, judging whether user identification information supplied from a terminal unit having the user identification information stored in memory of the terminal unit is coincident with the user identification information read from the recording medium; and

when it is judged that the user identification information supplied from the terminal unit is coincident with the user identification information read from the

recording medium causing the output unit to send to a server, the user identification information showing the coincidence, wherein

the server sends to the output unit a reference number based on the received user identification information; and

the output unit buries the received reference number into the data read from the recording medium and sends the data to the server.

27. (previously presented) The method according to claim 26, wherein:

when it is judged that the user identification information supplied from the terminal unit is coincident with the user identification information read from the recording medium, an encryption key is exchanged between the output unit and the server; and

the user identification information showing the coincidence is encrypted with the exchanged encryption key and sent to the server.

28. (previously presented) The method according to claim 26, wherein when it is judged that the user identification information supplied from the terminal unit is not coincident with the user identification information read from the recording medium, data read from the recording medium will not be sent.

29. (previously presented) The method according to claim 26, wherein when it is judged that the user identification information supplied from the terminal unit is not coincident with the user identification information read from the recording medium, a display is made on a display unit of an output unit to prompt a user to select other data recorded in the recording medium.

30. (previously presented) The method according to claim 26, wherein data sent from the output unit is stored in a storage unit provided in the server.

31. (previously presented) The method according to claim 26, further comprising steps of:

detecting whether the terminal unit is connected;

judging when the terminal unit is connected and whether the user identification information sent from the terminal unit is coincident with the user identification information read from the recording medium; and

decrypting data read from the recording medium when the user identification information sent from the terminal unit is coincident with the user identification information read from the recording medium.

32. (previously presented) The method according to claim 31, wherein when the terminal unit is connected, an encryption key is exchanged between the output unit and the terminal unit, and the user identification information read from the memory of the terminal unit is encrypted with the exchanged encryption key and sent from the terminal unit to the output unit.

33. (original) The method according to claim 31, wherein:

the output unit has an information holder to hold the user identification information sent from the terminal unit; and

when it is detected that the terminal unit is not connected, it is judged whether the user identification information read from the information holder is coincident with the user identification information read from the recording medium.

34-35. (canceled)

36. (previously presented) A method for controlling data recording, comprising the steps of:

upon request, sending data stored in a storage unit provided in a server, said data having at least buried therein user identification information intended to

identify a user and having been encrypted with the user identification information, to a recorder;

causing the recorder to extract the user identification information from the received data;

judging whether the extracted user identification information is coincident with user identification information held in an information holder provided in the recorder; and

recording the received data to a recording medium when the extracted user identification information is coincident with the user identification information held in the information holder provided in the recorder;

wherein when it is judged that the user identification information extracted from the received data is not coincident with the user identification information held in the information holder in the player, it is judged whether user identification information in the received data is to be rewritten;

wherein when it is judged that the user identification information in the received data is not to be rewritten, the received data is recorded to the recording medium.

37. (previously presented) The method according to claim 36, wherein when it is judged that the user identification information in the received data is to be rewritten, the recorder acquires the user identification information from the server, decrypts the received data, re-encrypts the decrypted data with new user identification information and records it to the recording medium.

38. (original) The method according to claim 37, wherein when it is judged that the user identification information in the received data is to be rewritten, the new user identification information is sent from the recorder to the server.

39. (previously presented) The method according to claim 37, wherein:

when it is judged that the user identification information in the received data is to be rewritten, the server judges whether the user identification information can be rewritten; and

when the user identification information can be rewritten, the recorder acquires the user identification information from the server.

40. (previously presented) The method according to claim 39, wherein the server judges, based on solvency of a grantee of the received data sent from the recorder, whether the user identification information can be rewritten.

41. (original) The method according to claim 39, wherein when it is judged that the user identification information cannot be rewritten, the recorder records the received data to the recording medium.

42. (previously presented) The method according to claim 37, wherein user identification information is acquired from the received data;

the received data is decrypted with the user identification information acquired from the received data; and

when the data has not successfully been recorded to the recording medium, the recorder deletes the received data.

43. (previously presented) The method according to claim 41, wherein:

the received data decrypted with the new user identification information is re-encrypted; and

when the re-encrypted received data has not successfully been recorded to the recording medium, the recorder sends a failure-in-storage signal to the server.

44. (previously presented) The method according to claim 37, wherein:

the received data decrypted with the new user identification information is re-encrypted; and

when the re-encrypted received data has successfully been recorded to the recording medium, a grantee of the received data is charged for the data thus recorded.

45. (previously presented) The method according to claim 43, wherein:

the received data decrypted with the new user identification information is re-encrypted; and

when the re-encrypted received data has successfully been recorded to the recording medium, the recorder supplies the server with a success-in-storage signal and a grantee of the received data is charged based on the success-in-storage signal.

46. (previously presented) The method according to claim 37, wherein:

a reference signal is additionally buried in data to be stored into the storage unit provided in the server; and

when it is judged that user identification information in the received data is to be rewritten, the recorder sends the reference signal to the server and the server will operate based on the received reference signal.

47. (previously presented) A data transmitting/receiving method, comprising the steps of:

when a recorder/player outputs data read from a recording medium having recorded therein data having user identification information intended to identify a user and which has been encrypted with the user identification information, judging whether the user identification information supplied from a terminal unit with a memory having user identification information recorded therein is coincident with the user identification information read from the recording medium;

when it is judged that the user identification information supplied from the terminal unit is coincident with the user identification information read from the

recording medium, causing the recorder/player to send to a server the user identification information showing the coincidence, wherein

the server sends to the recorder/player a reference number based on the received user identification information;

the recorder/player buries the received reference number into the data read from the recording medium, sends the data to the server and stores the data into a storage unit provided in the server; and

upon request, sending data stored in the storage unit provided in the server to the recorder/player, wherein

the recorder/player extracts the user identification information from the received data;

judging whether the extracted user identification information is coincident with the user identification information stored in the memory in the terminal unit; and

causing the recorder/player to record the received data to the recording medium when it is judged that the extracted user identification information is coincident with that stored in the memory of the terminal unit.

48. (previously presented) The method according to claim 47, wherein when it is judged that the user identification information supplied from the terminal unit is not coincident with the extracted user identification information read from the recording medium, ceasing reading of the data from the recording medium.

49. (previously presented) The method according to claim 47, wherein when it is judged that the extracted user identification information read from the recording medium is not coincident with the user identification information stored in the memory of the terminal unit, judging whether user identification information in the received data is to be rewritten.

50. (original) The method according to claim 49, wherein when it is judged that the user identification information in the received data is not to be rewritten, the recorder/player records the received data to the recording medium.

51. (previously presented) The method according to claim 50, wherein when it is judged that the user identification information in the received data is to be rewritten, the recorder/player acquires user identification information in the data sent from the server, decrypts the data received from the server, re-encrypts the decrypted data received from the server with new user identification information and records the data to the recording medium.

52. (previously presented) The method according to claim 51, wherein:

when it is judged that the user identification information in the received data is to be rewritten, the server judges whether the user identification information can be rewritten; and

when the user identification information can be rewritten, the recorder/player acquires user identification information from the data sent from the server.

53. (previously presented) The method according to claim 52, wherein the server judges, based on solvency of a grantee of the data sent from the recorder/player, whether the user identification information can be rewritten.

54. (original) The method according to claim 53, wherein when it is judged that the user identification information cannot be rewritten, the recorder/player records the received data to the recording medium.

55. (previously presented) The method according to claim 51, wherein user identification information is acquired from the received data;

the received data is decrypted with the user identification information acquired from the received data;

the decrypted received data is re-encrypted with new user identification information; and

when the received data has not successfully been recorded to the recording medium, the recorder/player deletes the received data that has not successfully been recorded.

56. (previously presented) The method according to claim 55, wherein:

the received data decrypted with the new user identification information is re-encrypted; and

when the re-encrypted received data has not successfully been recorded to the recording medium, the recorder/player sends a failure-in-storage signal to the server.

57. (previously presented) The method according to claim 51, wherein:

the received data decrypted with the new user identification information is re-encrypted; and

when the re-encrypted received data has successfully been recorded to the recording medium, a grantee of the received data is charged for the data thus recorded.

58. (previously presented) The method according to claim 57, wherein:

the received data decrypted with the new user identification information is re-encrypted; and

when the re-encrypted received data have successfully been recorded to the recording medium, the recorder supplies the server with a success-in-storage signal and the grantee of the received data is charged based on the success-in-storage signal.

59. (cancelled)